UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

A.P., a minor, by and through her guardian, CARLOS PENA, CARLOS PENA, RANDOLPH FRESHOUR, and VINCENZO ALLAN, each individually and on behalf of similarly situated individuals, *Plaintiffs*, v. CERENCE INC., a Delaware corporation, *Defendant.*	)	No. 1:23-cv-02667 Hon. Nancy L. Maldonado Magistrate Judge M. David Weisman

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT CERENCE INC.'S MOTION TO DISMISS SECOND AMENDED COMPLAINT

Dated: September 14, 2023

Myles McGuire
Paul T. Geske
Colin Primo Buscarini
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
pgeske@mcgpc.com
cbuscarini@mcgpc.com

Counsel for Plaintiffs and the putative class

I. INTRODUCTION

Defendant's voice recognition technology does more than merely understand words and phrases. It captures the unique sounds and features of users' voices—or voiceprints—for "identification and verification" purposes, to "understand who is speaking," and to "deliver advanced levels of personalization[.]" (Second Amended Class Action Complaint ¶ 28, Dkt. 24, hereinafter "Complaint" or "Compl."). Voiceprints, like fingerprints, are a type of "biometric identifier" expressly protected under Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.* However, Defendant made no attempt to comply with BIPA when it captured Plaintiffs' voiceprints here.

In Defendant Cerence Inc.'s Motion to Dismiss Second Amended Complaint (Dkt. 29, hereinafter the "Motion to Dismiss" or "Motion"), Defendant self-servingly attempts to deny that it ever collects or obtains voice biometrics, and—for Plaintiffs A.P. and Pena—deny that its technology uses protected voice biometrics at all. As shown in the Complaint, however, Defendant's own statements—in press releases, marketing materials, and public disclosures to investors—show that its voice recognition technology captures "voice biometrics" in order to identify users by voice and provide "personalized" responses. (Compl. ¶¶ 27-30). Given Defendant's own well-publicized descriptions of its products, Defendant cannot credibly deny the Complaint's well-pled allegations and advance an alternate narrative of its own making.

Nor may Defendant rewrite BIPA to add new terms that aren't in the statute's text. Specifically, Defendant incorrectly argues that Plaintiffs A.P.'s and Pena's voiceprints aren't protected under BIPA because they don't allege that they provided Defendant with other, additional identifying information, such as an address or phone number. (Mot. at 1). Put simply, there is no such requirement in the statute. Voiceprints—just like fingerprints—are capable of

being used to identify an individual and are protected "biometric identifiers" regardless of whether they are accompanied by other personal information about the user.

Defendant's arguments for dismissal of Plaintiffs' § 15(b) claims are likewise meritless. Defendant contends that its conduct is not subject to § 15(b) because it did not take an "active step" to collect Plaintiffs' voiceprints. (Mot. at 1-2). But the Complaint shows otherwise. Plaintiffs' well-pled allegations confirm that Defendant itself provided the automotive technology and software used to capture Plaintiffs' voiceprints, Defendant itself transferred and stored Plaintiffs' biometric data on its servers, and Defendant itself accessed the collected biometric data for its own benefit and to improve its products. Indeed, Defendant admits that it "capture[s] your voice and the words that you speak into the product" when "you use Cerence voice recognition technology[.]" (Compl. ¶ 30). In light of these well-pled facts, Defendant cannot pretend that it had no active role in the collection of Plaintiffs' voice biometrics.

Finally, Defendant asserts that all Plaintiffs' Section 15(d) claims are unsupported and based solely on "information and belief." (Mot. at 2). Defendant is wrong. Plaintiffs plead sufficient facts—corroborated through statements from Defendant itself—which plausibly establish that Defendant disseminates captured voice biometrics to "third-party datacenters" and "third-party public clouds." (Compl. ¶¶ 36, 39). As other courts in this District have found, this type of dissemination is a "textbook violation of § 15(d)." *Figueroa v. Kronos, Inc.*, 454 F. Supp. 3d 772, 785 (N.D. Ill. 2020).

Defendant's Motion to Dismiss should therefore be denied.

II. BACKGROUND

Defendant is a multinational technology company that provides voice assistant software and voice recognition technology for automobiles. (Compl. ¶ 23). Vehicles integrated with

Defendant's automotive technology employ advanced software and microphones placed throughout the vehicle's cabin to listen for and respond to spoken requests and commands from drivers and passengers. (*Id.* ¶¶ 25-26). Defendant's technology "listen[s] to almost every word and understand[s] practically any sentence relating to infotainment sector and vehicle operation," such as requests to play music, find destinations, or adjust seats and climate control settings. (*Id.* ¶ 1).

Not only does Defendant's technology understand spoken words, it also "uses 'voice biometrics – the identification and verification of a user based on the characteristics of their voice' to 'deliver advanced levels of personalization' and 'enable the automotive assistant to understand who is speaking, load their personal profile, authorize purchases by voice, and more.'" (*Id.* ¶ 28). With voice biometrics, Defendant's technology can "detect and isolate certain voices and filter out others," so that the automotive system can "identify[] the person who made a particular voice command" and where in the vehicle they are seated in order to "tailor [the system's] responses or actions to that specific person." (*Id.* ¶¶ 26, 31). Defendant's technology can also "identify who is speaking based on a memory of known speakers," which enables the software to retrieve "store[d] information about that speaker" from prior interactions. (*Id.* ¶ 29).

Defendant provides support for its in-car systems with its servers, third-party datacenters, and cloud-based services. (*Id.* ¶ 36). Defendant obtains, stores, and analyzes captured voice biometrics on its servers for the purpose of improving its voice recognition technology over time and aiding its in-car systems "in supplying responses to user queries or performing tasks." (*Id.* ¶¶ 36-38).

Plaintiffs in this matter are all individuals whose voiceprints were captured by Defendant through its automotive technology. Plaintiffs Allan's and Freshour's voiceprints were captured in Mercedes-Benz automobiles they owned and drove, and Plaintiffs A.P. and Pena had their

voiceprints captured while they were passengers in a Volkswagen automobile. (*Id.* ¶¶ 45-67).

Despite capturing and storing Plaintiffs' voiceprint biometrics, Defendant never informed Plaintiffs in advance that their biometrics were being collected or stored; never informed them of the specific purpose or length of time for which their biometrics were being collected, stored, and used; and never obtained consent or a written release from Plaintiffs prior to obtaining, disclosing, or disseminating their biometric data as required under Section 15 of BIPA. (*Id.* ¶¶ 4, 42, 45-67); *see generally* 740 ILCS 15(b), (d).

III. LEGAL STANDARD

Where a defendant moves for dismissal under Federal Rule 12(b)(6), the motion "tests only the legal sufficiency of the complaint," not the ultimate merits of the plaintiff's claims. *Hanley v. Green Tree Serv., LLC*, 934 F. Supp. 2d 997, 980 (N.D. Ill. 2013) (citing *Gibson v. City of Chi.*, 910 F.2d 1510, 1520 (7th Cir. 1990)). A complaint will survive a Rule 12(b)(6) motion as long as it "contain[s] sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A claim is plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* In other words, a plaintiff need only allege enough "to 'nudg[e]' his claim . . . across the line from conceivable to plausible." *McCauley v. City of Chi.*, 671 F.3d 611, 618 (7th Cir. 2011) (first alteration in original) (quoting *Iqbal*, 556 U.S. at 683).

When considering a Rule 12(b)(6) motion, the court must construe the complaint "in the light most favorable to the nonmoving party, accept well-pleaded facts as true, and draw all inferences in [the nonmovant's] favor." *Kolbe & Kolbe Health & Welfare Benefit Plan v. Med. Coll. of Wis.*, 657 F.3d 496, 502 (7th Cir. 2011). A complaint "should not be dismissed for failure to state [a] claim unless it appears beyond doubt that the plaintiff is unable to prove any set of facts

which would entitle the plaintiff to relief." *Supreme Auto Transp. v. Arcelor Mittal*, 238 F. Supp. 3d 1032, 1036 (N.D. Ill. 2017) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 546 (2007)).

IV. ARGUMENT

A. The Volkswagen Plaintiffs Sufficiently Plead That Defendant's Automotive Technology Captured Their BIPA-Protected Voiceprints.

Defendant attempts to deny that the voice and speech data it captured from Plaintiffs A.P. and Pena (the "VW Plaintiffs") are BIPA-protected biometric information, but its arguments are contrary to Plaintiffs' well-pled allegations and BIPA's express text. The Complaint describes in detail how Defendant's voice recognition technology utilizes voiceprints—"a biology-based set of measurements . . . that can be used to identify a person" based on their voice—which are by definition a type of "biometric identifier" protected under BIPA. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1093-94 (N.D. Ill. 2017); 740 ILCS 14/10.

The VW Plaintiffs' allegations do not merely parrot BIPA in a conclusory way. They thoroughly explain—with quotations from *Defendant's own descriptions* of its products—how Defendant's automotive technology "uses 'voice biometrics – the identification and verification of a user based on the characteristics of their voice' to . . . 'enable the automotive assistant to understand *who* is speaking[.]'" (Compl. ¶¶ 26-28, 46) (emphasis added); *Wilk v. Brainshark*, 631 F. Supp. 3d 522, 530 (N.D. Ill. 2022) (sustaining BIPA claims where the "[defendant]'s own marketing and resources confirms that its technology scans" biometrics).[1]

More specifically, one of the "core embedded" technologies in Defendant's automotive voice assistant is "speech signal enhancement," or SSE, which "isolate[s a speaker's] voiceprint from other ambient noise" in order "to accurately identify who in the car is talking." (Compl. ¶¶

[1] This statement from Defendant is not cabined to certain makes or models of automobiles, and instead broadly describes the capabilities of Defendant's voice recognition technology generally.

35, 46); (*see also id.* Figure 2) (stating that Defendant's system utilizes SSE for "speaker identification"). This functionality enables Defendant's technology to use a voiceprint to "identify the person who made a particular voice command and where they are [in the vehicle]," to provide a personalized response to the individual identified. (*Id.* ¶¶ 25-30). Importantly, when performing these functions, Defendant's SSE technology creates and utilizes spectrograms—a "visual graph used to display frequencies of sound waves"—from a person's voice. (*Id.* ¶¶ 33-35). Because these spectrograms are derived from an individual's voiceprint, they are a type of "biometric information" protected under BIPA. (*Id.* ¶¶ 20, 34-35); 740 ILCS 14/10.

These facts plausibly establish that "Defendant's technology mechanically analyzes [users'] voices in a measurable way such that [Defendant] has collected a voiceprint from Plaintiff[s] and other [users]." *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 517 (N.D. Ill. 2022). Indeed, "[t]he fact that [Defendant's] technology can effectively interpret and understand" queries and voice commands from specific individuals "shows that it detects and analyzes human speech in a way that a mere recording device does not." *Id.*

Defendant nonetheless contends that the VW Plaintiffs' voiceprint data cannot qualify as a "biometric identifier" within the meaning of BIPA because the VW Plaintiffs do not also allege that they provided Defendant with other "identifying information," such as a physical address or email address "to which Cerence could link" their biometrics. (Mot. at 8). However, there is no such requirement in BIPA.

Rather, BIPA defines "biometric identifier" with a "specific, one-by-one listing" that provides "the *complete* set of *specific* qualifying biometric identifiers." *Rivera*, 238 F. Supp. 3d at 1094 (emphases in original). Each item on this list—including a voiceprint—is "a biology-based set of measurements ('biometric') that can be used to identify a person ('identifier')." *Id.* Critically,

each listed biometric identifier is *capable* of identifying an individual even without other, additional identifying information. *Id.* By way of analogy, a fingerprint is capable of being used to identify a person even if the print isn't accompanied by a name and address. The same is true for a voiceprint. And both are equally protected under BIPA.

Accordingly, BIPA does not require Plaintiffs to allege that Defendant captured other, additional information beyond what's expressly listed in the statute. The Illinois legislature determined that voiceprints and other biometric identifiers are by themselves sensitive enough to warrant protection. 740 ILCS 14/5(c) ("Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse"); *Columbo v. YouTube, LLC*, No. 3:22-cv-06987-JD, 2023 WL 4240226, at *3 (N.D. Cal. June 28, 2023) (Donato, J.) ("[T]he Illinois legislature was perfectly free to define 'biometric identifier' in a specific manner[.]").

If instead Defendant's argument were adopted, it would allow companies to flagrantly capture and amass biometrics for any purpose, all while avoiding compliance with BIPA merely by choosing not to gather email or physical addresses. That's not what BIPA says, and it's clearly not what the Illinois legislature intended.

Given that Defendant's argument finds no support in BIPA's text, it's no surprise that numerous courts have already rejected the same argument in other cases. For example, in *Hazlitt v. Apple Inc.*, the plaintiffs brought BIPA claims against Apple for allegedly using its Photos application to collect facial geometry from users' photographs. 500 F. Supp. 3d 738, 742 (S.D. Ill. 2020), *vacated on other grounds, In re Apple Inc.*, 2021 WL 2451296 (7th Cir. 2021). Apple moved to dismiss, arguing that the facial data it collected from photos was "anonymous" and thus did "not qualify as biometric identifiers[.]" *Id.* at 748. The court rejected this argument as contrary to the statute. *Id.* As the court explained, the word "identifier" in BIPA "modifies the word

'biometric' to signal that the types of data listed"—including voiceprints—"*could* be used to identify a person" and are thus protected under BIPA even absent other personal information. *Id.*

Many other decisions are in accord with *Hazlitt* and have reached the same result. *See, e.g.*, *Rivera*, 238 F. Supp. 3d at 1095; *Columbo*, 2023 WL 4240226, at *3 ("In YouTube's view, biometric identifiers must identify a person and biometric information must actually be used to identify a person. . . . The point is not well taken. . . . YouTube's request to ignore the definition of 'biometric identifier' supplied by the Illinois legislature in favor of a single-minded focus on the word 'identifier' is misdirected"); *Melzer v. Johnson & Johnson Consumer Inc.*, No. 22-3149, 2023 WL 3098633, at * (D.N.J. April 26, 2023) (same); *see also Flores v. Motorola Solutions, Inc.*, No. 1:20-cv-01128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021) (holding that BIPA still applies even "where no relationship between the collector and the individual exists").

Defendant's Motion ignores the cases cited above and instead relies solely on *Daichendt v. CVS Pharm., Inc.*, No. 22 CV 3318, 2022 WL 17404488 (N.D. Ill. Dec. 2, 2022). However, *Daichendt* is an outlier. And notably, the *Daichendt* decision does not cite *any* authority in support of the notion that individuals' biometrics are not protected unless accompanied by additional identifying information. Regardless, to the extent the Court finds *Daichendt* persuasive, the VW Plaintiffs have in fact alleged that Defendant collected additional identifying information beyond just their voiceprints. (*See, e.g.*, Compl. ¶ 44) ("Cerence also collects and stores location data and other personally identifiable information when users engage with its platform.").[2]

In short, the VW Plaintiffs' well-pled allegations plausibly show that their voiceprints are capable of being used to identify them—just like their fingerprints—and fall within BIPA's express definition of biometric identifier. Their voiceprints are therefore protected under BIPA

[2] Defendant's Motion incorrectly states that Plaintiffs removed this allegation when they filed their Second Amended Complaint. Defendant is wrong.

even without additional, accompanying information.[3]

B. The Complaint Sufficiently Alleges That Defendant Obtained Plaintiffs' Biometrics Without Their Consent In Violation Of § 15(b) of BIPA.

1. Defendant actively captures users' voiceprint biometrics with its automotive technology.

All Plaintiffs state claims under § 15(b) of BIPA, because Defendant captured Plaintiffs' voiceprint biometrics without consent. Under § 15(b), private entities must provide advance notice and receive a signed release before they may "collect, capture, purchase, receive through trade, or otherwise obtain" an individual's biometrics. 740 ILCS 14/15(b). Because § 15(b) uses active verbs, some courts have held that § 15(b) only applies if the defendant took "some active step beyond mere possession" of the biometric information. *Ronquillo v. Doctor's Assocs., LLC*, 597 F. Supp. 3d 1227, 1231 (N.D. Ill. 2022). This "active step" requirement is not a high bar; a plaintiff need only allege enough facts to "allow for the reasonable inference that [the defendant] played more than a passive role in the process" to state a § 15(b) claim. *Id.* at 1232.

Here, the Complaint describes multiple ways that Defendant actively obtained Plaintiffs' biometrics. ***First***, Defendant directly captures voiceprint biometrics through its own automotive technology. (Compl. ¶¶ 26-30, 36-38). Indeed, Defendant admits "that [w]hen you use Cerence voice recognition technology, whether by using Cerence's own Products or by using third party products that employ Cerence voice recognition technology"—like the automotive voice assistants at issue here—"*we* may capture your voice and the words that you speak into the product." (*Id.* ¶ 30) (emphasis added and quotation marks omitted). And when Defendant "captures" a "voice," it

[3] Defendant notes in passing "that collection or storage of anonymized data is not" sufficient to confer Article III standing. (Mot. at 7-8). If the Court finds that Defendant anonymized the Volkswagen Plaintiffs' voice biometrics, and that this eliminates Article III jurisdiction, then the Volkswagen Plaintiffs' claims should be severed and remanded to state court rather than dismissed. (*See* Dkt. Nos. 12, 15, 16).

also captures the speaker's "voice biometrics" to "enable the automotive assistant to understand who is speaking[.]" (*Id.* ¶¶ 26-28). Each of the Plaintiffs allege that Defendant captured their voiceprint biometrics in this way. (*Id.* ¶¶ 45-67). The fact that Defendant directly captures users' voiceprints with its own technology is by itself sufficient to show "active" involvement. *King v. PeopleNet Corp.*, No. 21 CV 2774, 2021 WL 5006692, at *8 (N.D. Ill. Oct. 28, 2021).

Second, Defendant accesses the biometric data captured with its technology and sends that data to its servers. (Compl. ¶¶ 30, 36, 51, 58, 65). Specifically, Defendant's "software sends [captured biometric] data and information to and from its servers" to "aid Cerence's voice assistant technology and software in supplying responses to user queries or performing tasks." (*Id.* ¶ 36); (*see also id.* n.8) ("Both the head unit in the vehicle *and the server* evaluate the data and send a reply" to voice commands) (emphasis added)). Defendant's act of transmitting biometric data to its servers is another active step. *Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021) (plaintiff "sufficiently alleged an active step" where the defendant's system "store[d] users' biometric information both on the [biometric] device *and* in [the defendant]'s servers" (emphasis in original)); *Mayhall ex rel. D.M. v. Amazon Web Servs. Inc.*, No. C21-1473, 2022 WL 2718091, at *10 (W.D. Wash. May 24, 2022) ("Plaintiff's allegations plead an 'active step'" because "Defendants uploaded or otherwise stored the biometric data on their servers.").

Third, Defendant actively uses the captured voiceprint biometric data for its own purposes. These purposes include "creat[ing] usage statistics and improv[ing] its services" to make the voice assistant more effective at responding to user queries and commands. (Compl. ¶ 38). Defendant's "technology 'is constantly learning driver preferences based on previous commands and behaviuors [sic], making interaction with the assistant increasingly intuitive over time.'" (*Id.*). Defendant's use of Plaintiffs' biometric data is yet another active step. *See Kyles v. Hoosier Papa*

LLC, No. 1:20-CV-07146, 2023 WL 2711608, at *6 (N.D. Ill. March 30, 2023) (sustaining § 15(b) claims where the defendant "regularly downloads data" from the biometric system and "generates reports . . . based on the data it downloaded.")

Fourth, Defendant actively partners with automobile manufacturers to integrate its voice recognition technology in automotive systems. Defendant is not merely a passive participant in these partnerships; its technology is the *sine qua non* that "powers" the automotive voice assistants in its clients' vehicles. (Compl. ¶¶ 45, 54, 61). Without Defendant's active involvement, the voice assistants in Volkswagen and Mercedes-Benz automobiles could not operate as they do.

Despite the ample facts showing Defendant's direct and active involvement in the collection of users' voiceprint biometrics, Defendant nonetheless asserts that Plaintiffs haven't pled that Defendant "affirmatively 'did something' to collect their purported voiceprints." (Mot. at 10). But this argument improperly ignores most of Plaintiffs' well-pled allegations. Plaintiffs have alleged sufficient facts—supported with statements directly from Defendant—to plausibly establish that Defendant itself provided the automotive technology and software used to capture Plaintiffs' voiceprints, Defendant itself transferred Plaintiffs' biometric data to its servers, and Defendant itself obtained the collected biometric data, which it then used for its own purposes. Accordingly, the Complaint plausibly shows that Defendant "played more than a passive role in the" capture of Plaintiffs' voiceprint biometrics. *Ronquillo*, 597 F. Supp. 3d at 1232.

Defendant also argues that Plaintiffs don't provide enough "factual detail explaining *how* Cerence gained control of biometrics or 'collected' their biometric data." (Mot. at 10) (emphasis in original). At the pleadings stage, however, a "[p]laintiff need not show in granular detail the precise means by which users' biometric data travelled from [the defendant's] devices to [its] servers." *Heard*, 524 F. Supp. 3d at 840. In short, Defendant seeks to impose a heightened standard

where there is none. The Complaint's well-pled allegations are more than sufficient to meet the liberal pleading standard of Federal Rule 8.

2. Defendant itself obtained Plaintiffs' voice biometrics.

Finally, Defendant contends—solely as to Plaintiffs Allan and Freshour—that "it is '***the car***' (not Cerence)" that collected Plaintiffs' biometrics because Defendant's "voice biometric technology is ***embedded*** in the vehicles." (Mot. at 11) (emphases in original). However, "embedded" is just another way of saying that Defendant's voice biometric technology is integrated with other in-car technology and software. (Compl. ¶¶ 25, 41). This integration does not alter the fact that Defendant itself obtained Plaintiffs' voice biometrics with its own technology.

Nor does "embedded" mean that captured biometric data stays solely in the car. Defendant's "systems are designed to seamlessly shift data and compute resources *between the cloud and computer systems that are onboard vehicles*." (Compl. ¶ 36) (emphasis added). When a user makes a voice command or query, "[b]oth the head unit in the vehicle *and the server* evaluate the data and send a reply" to the user. (*Id.* n.8) (emphasis added). As such, Defendant's automotive technology "is not hermetically sealed within a [car]; users' biometric data flows back to [Defendant]'s servers . . . for analysis and support services." *Heard*, 524 F. Supp. 3d at 840.

Plaintiffs' allegations are therefore sufficient to show that Defendant itself—not just its clients' cars—obtained Plaintiffs' voice biometrics. *See, e.g.*, *id.* at 841; *King*, 2021 WL 5006692, at ** 2, 8 (concluding that "[the defendant], not its client[s], was doing the capturing and obtaining of [the plaintiff]'s biometric information," because the defendant's biometric-enabled devices "captured [user] data and transmitted it to defendant's cloud-based . . . systems, hosted on [its] servers"); *Smith v. Signature Sys., Inc.*, No. 2021-CV-02025, 2022 WL 595707, at *5 (N.D. Ill. Feb. 28, 2022) (concluding that the defendant itself, not its clients, collected the plaintiff's

biometric data because the "the data is stored in [the defendant's] electronic database.").

C. Plaintiffs' § 15(d) Claims Are Also Sufficiently Pled And Withstand Dismissal.

Section 15(d) generally prohibits private entities like Defendant from disclosing or disseminating biometrics in their possession without the subjects' informed consent. 740 ILCS 14/15(d); *Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604, 610 (N.D. Ill. 2020). Plaintiffs' Complaint establishes that Defendant both: (1) gained possession of Plaintiffs' voice biometric data after capturing it; and (2) unlawfully disseminated that data to third-parties without consent.

1. Defendant possesses voice biometric data on its servers.

Defendant gained possession of Plaintiffs' biometric data when it transferred that data to its own servers. Although BIPA doesn't define the term "possession," numerous courts have held that where, as here, a private entity stores biometric data on its servers or datacenters, it is "in possession" of that data under BIPA. *See, e.g., Naughton v. Amazon.com, Inc.*, No. 20-cv-6485, 2022 WL 19324, at *4 (N.D. Ill. Jan. 3, 2022) (sustaining § 15(d) claims where the defendant "store[d] [the plaintiff's] biometric data in a database. This plainly satisfies the 'possession' requirement at the pleadings stage."); *Doe ex rel. Doe v. Apple Inc.*, No. 3:20-CV-421-NJR, 2022 WL 17538446, at **5-6 (S.D. Ill. Aug. 1, 2022) (plaintiffs sufficiently alleged possession where the defendant's technology "automatically transfers . . . data derived from faceprints[] to [its] servers via the cloud" and then stores that data "on [its] servers."); *Smith*, 2022 WL 595707, at *4.

As explained above, when Defendant's automotive technology captures biometric data, the data *does not* simply remain on the cars' operating systems; rather, Defendant's technology transmits the captured data to Defendant's servers—both for storage and to aid the voice assistant in responding to user commands. (Compl. ¶¶ 30, 36-39); *Mayhall*, 2022 WL 2718091, at *12 (sustaining § 15(d) claims where the defendants "moved [the biometric data] to, or stored it in,

different server locations across Defendants' server infrastructure."). And the fact that Defendant has full access to and control over the data on its servers further demonstrates its possession. (Compl. ¶¶ 36-38) (asserting that Defendant uses captured data to, among other things, respond to user queries, "create usage statistics and improve its services."); *see Kyles*, 2023 WL 2711608, at *4 (holding that the plaintiff sufficiently pled possession where the defendant "retains access to the [biometric] system, and regularly downloads and uses data from it.").

Defendant contends that Plaintiffs cannot show possession because Defendant's "voice biometric technology is ***embedded*** in [the Plaintiffs'] vehicles." (Mot. at 13) (emphasis in original). As already explained above, however, this argument is belied by Plaintiffs' well-pled allegations. (Compl. ¶¶ 30, 36-37). Defendant's automotive technology is not a closed system; the "users' biometric data flows back to [Defendant]'s servers," which shows that Defendant was "plausibly 'in possession' of users' biometric data." *Heard*, 524 F. Supp. 3d at 540.

2. Defendant unlawfully disseminated Plaintiffs' biometrics to third-party data storage vendors and content providers.

Consistent with Federal Rule 8, BIPA plaintiffs bringing Section 15(d) claims need only allege "plausible dissemination," *Naughton*, 2022 WL 19324, at *4, and Plaintiffs' Complaint here readily meets this standard. The Complaint establishes that Defendant unlawfully disseminates collected biometric data to third-party data storage and cloud services providers. (Compl. ¶ 36) (biometric data that Defendant collects is "hosted at datacenters belonging to third parties."). Defendant "use[s] multiple data centers and cloud hosting to provide the compute power for [its] products," and Defendant "splits the data it collects 'between onsite server rooms and two third-party data centers.'" (*Id.* ¶¶ 36, 39) ("information that Cerence [automobile] 'customers use is hosted in third-party public clouds'"). This is a "textbook violation of § 15(d)." *Figueroa*, 454 F. Supp. 3d at 785 (sustaining § 15(d) claims where "[the defendant] disseminated Plaintiffs'

biometric data to other firms that hosted the information in their data centers."); *Trio v. Turing Video, Inc.*, No. 21-cv-04409, 2022 WL 4466050, at **1, 12 (N.D. Ill. Sept. 26, 2022) (sustaining § 15(d) claims against entity that "transmitted [biometric data] to [the defendant's] servers and other third parties who host that data").

Further, Plaintiffs also plausibly allege that Defendant unlawfully disseminates biometrics to third-parties when carrying out user requests. Defendant's "in-car technology interfaces with and has access to many external content services that it utilizes to respond to voice commands," such as requests to "provide navigation routes, make purchases, and play music through music streaming applications." (Compl. ¶¶ 28, 40). It is therefore plausible that Defendant discloses or disseminates users' biometric data when interfacing with these third-party platforms.

Defendant attempts to find fault with Plaintiffs' Section 15(d) claims, arguing that they are based on mere "information and belief." (Mot. at 12-13). But Plaintiffs' Complaint contains numerous well-pled facts showing dissemination—nearly all of which *aren't* pled on information and belief—that support and substantiate their § 15(d) claims. And, in any event, "[t]he *Twombly* plausibility standard . . . does not prevent a plaintiff from pleading facts alleged upon information and belief where the facts are peculiarly within the possession and control of the defendant." *Cothron*, 467 F. Supp. 3d at 618. That is the case here, because Defendant did not inform Plaintiffs that their biometrics were being disseminated—or obtain their consent—prior to doing so. *Id.*

In sum, Plaintiffs' Complaint sufficiently pleads "plausible dissemination" with well-pled facts about the circumstances where dissemination occurs and the types of third-parties that Defendant disseminates biometric data to. *Id.* "The law does not demand more at the pleadings stage," so Plaintiffs' Section 15(d) claims should be sustained. *Id.*

V. CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss should be denied in its entirety.[4]

Dated: September 14, 2023

Respectfully Submitted,

A.P., a minor, by and through her guardian, CARLOS PENA, CARLOS PENA, RANDOLPH FRESHOUR, and VINCENZO ALLAN, each individually and on behalf of similarly situated individuals

By: /s/ *Paul T. Geske*
One of Plaintiffs' Attorneys

Myles McGuire
Paul T. Geske
Colin Primo Buscarini
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
pgeske@mcgpc.com
cbuscarini@mcgpc.com

Counsel for Plaintiffs and the putative class

[4] In the event that the Court grants Defendant's Motion in whole or in part, Plaintiffs request that any such dismissal be made without prejudice to provide Plaintiffs with an opportunity to correct any curable defects, as it is well established that a complaint should not be dismissed for failure to state a claim unless it is clear that the plaintiff is unable to prove any set of facts which would entitle the plaintiff to relief. *See supra* p.5.

CERTIFICATE OF SERVICE

I, the undersigned, certify that on September 14, 2023 I filed the foregoing *Plaintiffs' Memorandum of Law in Opposition to Defendant Cerence Inc.'s Motion to Dismiss Second Amended Complaint* with the Clerk of Court using the Court's CM/ECF system, which will cause a copy of said document to be electronically transmitted to all counsel of record.

By: /s/ *Paul T. Geske*
Paul T. Geske